

JED:TD  
F.#2007R00950

**M-07 942**

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

: **AFFIDAVIT IN SUPPORT**  
: **OF ARREST WARRANT**

- against -

:

ROMAN VEGA,

:

also known as

"Boa", "Roman Stepanenko"

:

"Randy Rioluta," and

ICQ User No. 107711,

:

Defendant.

:

- - - - - X

EASTERN DISTRICT OF NEW YORK, ss.:

HARI NOTANI, a Special Agent of the United States  
Secret Service ("Secret Service"), deposes and says:

On or about and between October 2002 and February 26,  
2003, both dates being approximate and inclusive, in the Eastern  
District of New York and elsewhere, the defendant ROMAN VEGA,  
also known as "Boa", "Roman Stepanenko," "Randy Rioluta" and ICQ  
User No. 107711, together with others, did knowingly and with  
intent to defraud conspire to effect transactions with one or  
more access devices issued to another person or persons, to wit:  
credit card account numbers and the subcomponents thereof,  
including bank identification numbers, credit card verification  
codes, and credit card personal identification numbers, to  
receive payments or other things of value during a one-year

period, the aggregate value of which was equal to or greater than \$1,000, in a manner affecting interstate commerce, in violation of Title 18, United States Code, Section 1029(a)(5).

(Title 18, United States Code, Section 1029(c)(1)(A)(ii)); and furthermore,

On or about and between October 2002 and February 26, 2003, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendant ROMAN VEGA, also known as "Boa", "Roman Stepanenko," "Randy Riolta" and ICQ User No. 107711, together with others, knowing that the property involved in financial transactions, to wit: United States currency, represented the proceeds of some form of unlawful activity, did knowingly and intentionally conspire to conduct such financial transactions affecting interstate and foreign commerce, with the intent to promote the carrying on <sup>of</sup> some specified unlawful activity, to wit: conspiracy to engage in access device fraud, in violation of Title 18, United States Code, Sections 1029(b)(2) and 1029(c)(1)(A)(ii) ~~of said specified~~ <sup>unlawful activity</sup> in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Section 1956(h))

The basis of my information and the grounds for my belief are as follows:

1. I am a Special Agent with the Secret Service, and I have been involved personally in the investigation of this matter. I have been a Special Agent for over five years and am presently assigned in New York to the Electronic Crimes Task Force, coordinated by the Secret Service. I have participated in dozens of arrests and searches involving computer crimes and money-laundering, and I have investigated over 20 cases involving computer intrusions, theft of personal identifying information and other computer-based crimes as well as related money-laundering.

2. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including interviews I have conducted, my examination of reports and records, and my conversations with other law enforcement officers. Because this affidavit is being submitted for the limited purpose of establishing probable cause to arrest, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part.

**I. The Credit Card Industry And  
Credit Card Fraud Terminology**

3. Credit card companies, such as Visa, and banks and others that issue cards ("card issuers"), have developed common standards and associated terminology that enable credit cards

readily to be used throughout the world, across banking systems and over the Internet. The following are standard terms used by legitimate participants in the credit card industry:<sup>1</sup>

- **BIN** is an acronym for "bank identification number." Each bank, including any bank that issues credit cards, is assigned a unique BIN. Any valid credit card number includes the BIN of the card's issuer.<sup>2</sup>
- **"Card Present" and POS Transactions.** Typically, credit card companies require any merchant who deals face-to-face with a customer who pays by credit card to read the magnetic stripe to confirm the presence of several forms of authenticating information (see below). Such transactions are known as "card present" transactions. "POS" stands for "point of sale" and refers to the large subcategory of "card present" transactions in which merchandise is charged via POS terminals, which are essentially cash registers integrated into a merchants' sales-reporting and credit card charging information systems.
- **CVV1** is an acronym for "Card Verification Value 1." CVV1 is a numeric code that a credit card issuer assigns to a card holder in order to deter fraud in connection with "card present" transactions. The CVV1 does not appear on the face of the card, but rather, is encoded in the card's magnetic stripe. Most credit card issuers will not accept a "card present" charge unless the information that a merchant obtains from swiping the card in a magnetic stripe reader includes the CVV1. Accordingly, in order to forge a stolen

---

<sup>1</sup> For the purposes of the instant discussion, the term "credit card" refers not only to traditional credit cards, but also to debit cards.

<sup>2</sup> Like the other credit card information discussed below, BINs are of interest to credit card thieves. BINS enable thieves to target more vulnerable financial institutions and to spread thefts across a wide range of institutions, thereby reducing the risk of detection

credit card that can be used in "card present" transactions, a thief must possess not only the card number on the face of the card, but also the CVV1 encoded on the stripe.<sup>3</sup>

- **Track Data** refers to the categories of information encoded on the magnetic stripe of a credit card. Under a common industry standard, credit card issuers format the stripe into three separate "tracks," reserved for certain categories of information identifying the account holder and card issuer. Tracks 1 and 2 combined will always contain credit card account numbers, and will often contain other identifying information, often in encrypted form, such as the customer's name, BIN, and CVV1 code (see above).

4. As the options for use of credit cards have expanded, so has the potential for credit card fraud. There is now a worldwide market for stolen credit card information, much of it obtained through intrusions into the computer systems of providers of credit card services as well of the computers of individual cardholders.<sup>4</sup> Many of the thieves, (including, as

---

<sup>3</sup> It is increasingly common for sales transactions to be paid by credit card without cards being physically presented to the accepting merchants. The growth in these "**card not present**" transactions is largely due to the huge expansion in sales of merchandise over the Internet. To deter fraud when a card is used but not present, many major credit card companies (e.g., Visa and Mastercard), have added a second card verification value ("**CVV2**"), usually consisting of 3-4 digits, which appears only on the face of the card.

<sup>4</sup> A carder may conduct the theft himself or pay others for doing or having done so. The theft may be perpetrated, for example, by hacking into the information system of credit card company or processor, by mass infection of cardholders' computers with data-mining "viruses" or by bribing employees of merchants to take unauthorized readings of a credit card at the same time as the employees swipe the cards with authorization through POS terminals.

described below, the defendant ROMAN VEGA) are well-versed in the above terminology and the underlying practices of the credit card industry. Thieves who steal large volumes of this credit card information and sell it are known as "**carders**." Carders often collude with each other in "**carding**" organizations, through which they sell the stolen information in bulk to others, who use it to make fraudulent credit card charges.

5. Carders have developed their own shorthand to describe the stolen information that they sell in bulk. A "**dump**" is carder shorthand for an electronic record containing the data from the magnetic stripe of a particular credit card, including at least Track 2 data, and sometimes Track 1 Data as well. "**Dumps**" refer to such records that a carder has misappropriated in bulk and sells in bulk. A buyer of dumps can thereupon copy them onto forged credit cards with which to make unauthorized "card present" charges and unauthorized ATM withdrawals.

## II. **Probable Cause For Arrest**

6. The defendant ROMAN VEGA is a citizen of the Ukraine, who for many years resided in the United States. In February 2003, authorities in Cyprus arrested VEGA and seized a Sony VAIO laptop computer (the "Subject Laptop Computer") from him. Thereafter, Cypriot authorities made the contents of the Subject Laptop Computer available for copying and use by

authorities in the United States. As detailed in part (A) below, there is probable cause to believe that an individual using and answering to the pseudonym "Boa" and ICQ number 107711 (further explained below) was a leading participant in the conspiracy to commit access device fraud and related money-laundering that is the subject of this affidavit. The evidence thereof includes but is not limited to evidence recovered from the Subject Laptop Computer. As demonstrated in part (B), below, VEGA, "Boa" and the user of ICQ number 107711 are one and the same person, as is demonstrated by evidence that includes but is not limited to evidence from the Subject Laptop Computer.

**A. BOA and ICQ No. 107711**

**--Shadowcrew Investigation**

7. From in or about October 2003 to October 2004, the Secret Service conducted an undercover investigation into a carding organization that operated by means of a website at [www.shadowcrew.com](http://www.shadowcrew.com) (the "Shadowcrew Carding Site"), which was accessible only to trusted sellers and buyers of stolen personal information. The investigation culminated in the arrest and conviction of approximately 30 individuals. During the course of the investigation, the Secret Service conducted court-authorized searches of Shadowcrew records, including records of messages that an individual had posted under the username "Boa," listing

the return e-mail address "info@factorymanagement.com." Those postings included the following summarized below:

a. On or about November 11, 2002, "Boa" posted a message protesting that another participant in the Shadowcrew Carding Site, a competing trafficker of dumps known as "BigBuyer," had placed Boa and his organization at risk of being apprehended by law enforcement. Specifically, Boa complained that "BigBuyer" had posted on the site the address of a "P.O. Box" that Boa maintained in the United Arab Emirates ("U.A.E.") "linked to physical address [sic]." Boa emphasized that he had been "compelled to supervise the urgent evacuation of [that] drop," since "this board we read not only [us], but also FBI and other special services like CID [criminal investigative division] from U.A.E." (meaning the board is not only read by participants but also scrutinized by the FBI in the U.S. and law enforcement in the U.A.E.). By contrast, as Boa also explained, he had organized his carding operations to safeguard both illicit sellers and illicit buyers:

All clients know, that addresses should be confidential which they give sellers for delivery of the goods. At Boa Factory all addresses are destroyed from a computer right after shipping order out. All of us do criminal business. How many people have informed the addresses to BigBuyer? Be not surprised, if FBI will go to your home. You are ready to evacuation [sic]? You have money to [sic] the lawyer?

(emphasis added)

b. On November 14, 2002, "Boa" made two more posts to the Shadowcrew Carding Site. In the first, Boa pledged that anyone who "post[s] any of our product's scans [sic]" on the site ("or somewhere else") "will be on the Boa Factory BLACK LIST [sic] forever." In the second, Boa stated that for "new cards we will accept [sic] only bulk orders" (meaning orders for credit cards in bulk) and that because Boa Factory was not "planning to sale out [sic] new cards embossed" (i.e., forged cards embossed with the names and account numbers of the victim cardholders), buyers should "try to look around for your own embossers."

c. In a post dated December 25, 2002, "Boa" announced that buyers on the Shadowcrew Carding Site could henceforth buy from him two ways. "We recommend to take our dumps" (i.e., buy the dumps that Boa procured) through intermediaries "Gollum . . . or Script, as before " he wrote, but added that "[n]ow it is possible to buy the dumps directly at Boa Factory," at the website "www.boafactory.to." Boa added "[y]ou buy from us only the 100% efficient dumps with the first and second tracks at the price of the second track and 1-48 hours order processing." In other words, Boa was offering for sale dumps containing the Track 2 data essential to credit card fraud, with the Track 1 data offered for free to attract customers.

d. On December 28, 2002, "Boa" made two posts to the Shadowcrew Carding Site. The first endorsed "Credit cards with changeable billing address from Script." Praising the contraband marketed by "Script," Boa emphasized that "Script's cards are works [sic]. Highly recommended [sic]." In the second post, Boa announced that he was offering "Visa Credit Platinum cards from Cristmas shoppers [sic]. He added that the dumps were all "workable," included "both tracks" (i.e., Tracks 1 and 2), came from "different banks" -- and had "[j]ust [been] taken off from the processing centre" (meaning had just been stolen from a credit card processor).

--Evidence From The Subject Laptop  
Computer And Related Sources

8. On or about February 26, 2003, police in Nicosia, Cyprus, arrested the defendant ROMAN VEGA on credit card fraud charges. In the course of the arrest, Cypriot police also seized the Subject Laptop Computer from the hotel room where VEGA was staying. In March 2003, in Nicosia, with the permission of Cypriot authorities, special agents of the U.S. Secret Service and U.S. Postal Inspection Service imaged the hard drive of the Subject Laptop Computer, using established forensic principles, and took permanent possession of the entire computer. In the meantime, after his release by Cypriot authorities, VEGA came to

the United States, where he is now in federal custody awaiting sentence in the Northern District of California on related but separate charges to those that are the subject of this affidavit.<sup>5</sup>

9. The Secret Service has conducted a forensic examination of the imaged hard-drive of the Subject Laptop Computer seized from VEGA. The examination resulted in the recovery of text files that contained thousands of credit card numbers and related information. For example, within a folder labeled "Dumps" and a subfolder labeled "Script" -- the online nickname of the coconspirator identified in the Carder Planet investigation -- agents recovered two text files dated December 30, 2002, one of which contained Track Data for approximately 799 Visa credit cards and the other of which contained Track Data for approximately 545 credit cards issued by

---

<sup>5</sup> VEGA was prosecuted and convicted in Cyprus, where he remained in jail until approximately May 6, 2004. On or about May 6, 2004, VEGA was detained in Cyprus pursuant to a provisional arrest request by the United States Attorney for the Northern District of California, which had charged him with wire fraud and access device fraud. On or about June 3, 2004, VEGA, accompanied by U.S. Marshals, flew from Cyprus to Minneapolis, Minnesota. In federal court in Minneapolis, VEGA waived objection to extradition from Cyprus to the United States. He has since remained in federal custody on the Northern District of California charges. In November 2006, VEGA pleaded guilty in the Northern District of California to twenty counts of wire fraud, stemming from fraudulent Visa credit card transactions effected in January, February and March 2003. VEGA's sentencing on the latter charges is scheduled for August 28 or 29, 2007. It is anticipated that VEGA will be sentenced in that case to time served. In addition to the arrest warrant sought herein, an immigration detainer has been filed against VEGA.

MasterCard.<sup>6</sup> From the same forensic examination, agents recovered hundreds of e-mail messages and thousands of pages of ICQ "chats"<sup>7</sup> concerning carding transactions, embedded within many of which was detailed Track Data.

10. Virtually all of the e-mail exchanges, including those summarized below, are ones to which "Boa," using the e-mail addresses, "boa-factory@bk.ru," "boafactory@canada.com," and "boa@boafactory.com," was party. In addition, with respect to outbound messages from the latter two e-mail addresses that were recovered from the Subject Laptop Computer, most appear to have appear to have originated from that device, since (a) (in contrast to the inbound e-mails) they lack any Internet Protocol path ("IP header") information that would indicate those messages originated from outside that device and (b) most of the same outbound messages, including all of those summarized below, were recovered from a folder labeled "\boa@boafactory.com\trash" within an e-mail program within the Subject Laptop Computer,

---

<sup>6</sup> On or about January 13, 2003, an individual residing in Astoria, Queens, whose card number is among those contained in the list of 799 Visa dumps, complained to the issuer of the underlying card (Wachovia Bank) that he had been the victim of credit card fraud.

<sup>7</sup> ICQ (a pun on the expression "I Seek You.") is an instant message system maintained by America Online that has millions of users worldwide. Each ICQ user is assigned a unique numeric address. ICQ allows users to chat online in real time, send messages and files and exchange web page addresses.

indicating that "Boa" had used the same device both to create and delete those messages.

11. The ICQ chats recovered from the Subject Laptop Computer likewise appear to have been generated by that device in the course of its use by the defendant. All of the recovered ICQ chats were found in discrete folders within the Subject Laptop Computer reserved for recording ICQ exchanges while the user of that device was in conference with one or more other ICQ users. Moreover, virtually all of the recovered ICQ chats, including those summarized below, were ones to which a person using ICQ number 107711 was party. As detailed at Point II(B), evidence recovered from the ICQ chats demonstrates that "Boa," the user of ICQ number 107711 and the defendant ROMAN VEGA are one and the same person.

12. The following evidence with respect to e-mail messages and ICQ chats recovered from the Subject Laptop Computer is submitted as additional proof of the participation by the defendant ROMAN VEGA, also known as "Boa", "Roman Stepanenko," "Randy Riolta" and ICQ User No. 107711, in a conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(c)(1)(A)(ii), and to establish as well that the conspiracy's objectives also included engaging in financial transactions designed to promote access device fraud,

in violation of Title 18, United States Code, Section  
1956(a)(1)(B)(i):

a. **October 9-11, 2002 e-mail exchange between Boa "Klyvka" and "Den."** The three parties discussed payment to Boa for stolen credit card data. Boa approved Den's proposal to wire him \$950 using DeutscheBank in New York as an intermediary to wire money to Parex Bank in Vilnius, Lithuania (hereafter "to Parex-Vilnius through DeutscheBank-New York"). In the same exchange, Boa confirmed that he had received the payment from Den.

b. **November 7-8, 2002 e-mail exchange between "Script" and Boa.** On November 7, 2002, Script e-mailed a request to Boa for assistance in obtaining access to credit card information. On November 8, 2002, Boa e-mailed a response to Script.<sup>8</sup> Boa's response included 12 pairs of usernames and passwords ("login pairs"). Boa explained that each such pair enabled access to a different account of an credit card issuer at a credit card processor named Electronic Clearing House ("ECH"). Boa stated that he had already used these login pairs to access ECH's information systems and expected soon to receive additional pairs, which he also intended to forward to Script. Boa

---

<sup>8</sup> Although Script had sent his e-mail to "Boa" at trade@gmx.co.uk (other evidence of which was also found on the Subject Laptop Computer), Boa replied in this and subsequent responses from boa-factory@bk.ru.

emphasized that by means of such access, a user (such as him or Script) could confirm the validity of as many as 10,000 dumps in five minutes, without triggering suspension of the underlying credit cards. Boa also advised that he had sent Script a counterfeit credit card for examination. Later on November 8, 2002, Script replied that he had successfully used the login pairs that Boa had thus far provided, selling some of the dumps thereby confirmed and using others himself. Boa responded still later on November 8, 2002, offering to sell Script additional dumps.

c. **November 9-17, 2002 e-mail exchange between "Script" and Boa and supporting files.** On November 9, 2002, Script requested more dumps of Visa Classic credit cards from Boa. The same day, after Boa inquired how many dumps Script wanted, Script responded that he needed a few hundred and would pay Boa for them through the online money transfer service [www.webmoney.ru](http://www.webmoney.ru) ("WebMoney"). On November 11, 2002, after Boa e-mailed Script to offer several thousand such dumps, Script countered with a request that Boa supply 500 Mastercard dumps and 500 Visa Classic dumps, along with a few Gold and Platinum card dumps. On November 14, 2002, Script e-mailed Boa and confirmed that he had received more dumps. On November 16, 2002, Script e-mailed Boa. Script advised that he already sold 100 of the Visa Classic dumps. Script also complained that Boa had yet to

deliver the Visa Gold and Platinum card dumps. In addition, Script proposed to pay via WebMoney for the dumps that Boa had provided and accordingly, asked Boa to provide the details of his WebMoney account. On November 17, 2002, Boa sent his WebMoney account information to Script and also promised to send at least 100-200 Visa Gold and Platinum card dumps. Notably, among the other data that agents recovered from the Subject Laptop Computer was a compressed archive file dated 11/19/2002 that indicates Boa made good on the later promise. The archive contains three text files, labeled, respectively "Script-Gold.txt," "Script-Platinum.txt," and "Script-business.txt," which contain Track Data for a total of approximately 184 Visa Gold and Platinum credit cards.

d. **November 21, 2002 e-mail from Boa to Paul Shenon.** In this e-mail, Boa confirmed that he was offering to sell Shenon 300 counterfeit checks for \$28 each, plus shipping (total: \$8,420). Boa instructed Shenon to wire money to Parex-Vilnius through DeutscheBank-New York, unless Shenon wished to pay in euros, in which case, Boa offered to accept payment through an account at DeutscheBank in Germany.

e. **December 6-9, 2002 e-mail exchange between Script and Boa concerning, among other things, compromised credit cards of EDNY residents:**

- On December 6, 2002, Script e-mailed Boa stating that he had transferred \$300 to Boa's Webmoney account and

was seeking to buy an additional 1000 Gold and Platinum dumps, provided that Boa could assure that the underlying cards had been issued by a variety of banks (see note 2 above);

- Later on December 6, 2002 Boa replied, asking Script to confirm how many dumps Script sought to purchase;
- On December 7, 2002, Boa sent Script an e-mail containing another password pair for Script to use to access ECH and verify dumps. Boa also advised that he would no longer provide Script with credit card information for cards issued by Bank of America and instead provide him information on cards issued by other banks. The reason for the exchange, Boa explained, was that Bank of America had discovered that its systems had been hacked and therefore was moving to replace the compromised cards with secure ones. Boa added that he had an entire team of hackers focused on European processing centers, so he would soon be able to offer large quantities of European credit card dumps for sale. In addition, Boa wrote that he would like to refer to Script any retail buyers of simple credit card numbers with CVV codes and asked Script to provide the text of terms and conditions for sale of this data, which Boa would post on his new "Factory" website.
- Later on December 7, 2002, Script e-mailed Boa to confirm that Boa could use the text of advertising copy that Script had already posted at the Shadowcrew website (see above), so long as Boa modified it to set the minimum at 200 credit cards per sale. Script also thanked Boa for the new ECH login pair, explaining that the pairs that Boa had previously supplied had stopped working. Still later on December 7, 2002, Boa e-mailed 100 Visa Gold credit card dumps to Script.
- On December 9, 2002, Boa e-mailed Script a total of 100 dumps relating to Visa Gold and Platinum cards issued by a number of different banks. Subsequent investigation has revealed that soon thereafter, two cardholders, both of whom resided in Queens, New York and both of whose card numbers were within the 100 dumps, complained to the cards' issuer (on or about December 21, 2002<sup>2015</sup> and January 22, 2003, respectively) that they had been victimized by persons making unauthorized charges on their cards.

f. **December 21-28, 2002 e-mail exchange between Boa and "Izabela Brant," concerning, among other things, a compromised credit card issued by Lake Success, NY-based bank to Brooklyn cardholder.** On December 28, 2002, Boa received an e-mail from Brant. Brant asked Boa to supply her with dumps as well as white plastic (suitable for use in forging credit cards). On December 28, 2002, Brant sent an additional e-mail to Boa, this time including a tracking number for a Western Union money transfer that she stated that she had sent from New York City under the alias "Anna Semyonov" as payment to Boa for dumps. The same day, Boa sent Brant a reply e-mail in which he included Track Data for 12 different credit cards.<sup>9</sup> On December 31, 2002, Boa sent another e-mail to Brant that included Track Data for fifteen more credit cards.

---

<sup>9</sup> Further investigation has revealed that on December 27, 2002, a person using the name "Anna Semyonov," submitted \$500 at a Western Union outlet in Jackson Heights, Queens to be picked up ~~by~~ at any other Western Union location in the world by a person submitting identification in the name "Oskana Silva." Further investigation has also revealed that one of the twelve compromised credit card accounts whose identifiers Boa sent to Brant is (a) a Mastercard account issued by Astoria Federal Savings and Loan Association, maintained at that bank's headquarters in Lake Success, Nassau County, New York, for the benefit of (b) a cardholder who resided in Brooklyn.

g. **January-February 2003 ICQ exchanges between  
ICQ User No. 107711 and "Kent" a/k/a "Amanda."**

- On January 13, 2003, an individual using ICQ User Identification Number 59130832 (who in other communications identified him or herself as "Kent" and "Amanda") ("Kent/Amanda") sent ICQ User No. 107711 (i.e., as further established below, the defendant VEGA) an order via ICQ for dumps containing information on 134 Visa Signature cards. On or about January 13, 2003, ICQ user No. 107711 instructed Kent/Amanda that a payment of \$8,162.00 should be wired for his benefit to Parex-Vilnius through DeutscheBank-New York, in care of a Cyprus-based company (hereafter "wired for his benefit to the Cypriot account at Parex-Vilnius through DeutscheBank-New York").<sup>10</sup> On or about January 13, 2003, via ICQ, Kent/Amanda informed ICQ user No. 107711 that the money had been sent as directed.
- On or about January 28, 2003, via ICQ, Kent/Amanda, who indicated that he/she was based in Malaysia, placed a new order with ICQ User No. 107711, requesting dumps from credit card issuers based in Japan, Hong Kong, France and Switzerland. On or about January 28, 2003, ICQ User No. 107711 instructed Kent/Amanda that an initial payment of \$10,000 for these dumps should be wired for his benefit to the Cypriot account at Parex-Vilnius through DeutscheBank-New York. On or about January 29, 2003, Kent/Amanda advised ICQ User No. 107711 that the \$10,000 had been sent as directed.
- On or about February 2, 2003, Kent/Amanda ordered over 1,000 additional dumps from ICQ User No. 107711, at a total price of \$91,356. In his response on February 4, 2003, ICQ User No. 107711 instructed Kent/Amanda that a partial payment of \$12,001 should be wired for his benefit to the Cypriot account at Parex-Vilnius through DeutscheBank-New York.

---

<sup>10</sup> Thus, "Boa" and ICQ User No. 107711 were using the same circuitous route between, among other places, New York and Lithuania, to move money.

- On or about February 8, 2003, Kent/Amanda informed ICQ User No. 107711 that he/she needed 200-300 more dumps, to be delivered via encrypted email. On or about February 9, 2003, ICQ User No. 107711 stated that he had sent Kent/Amanda about 330-350 workable dumps, as requested. On or about February 9, 2003 and February 10, 2003, ICQ User No. 107711 instructed Kent/Amanda that a total of \$14,998, in installments of \$5,000 and 9\$9,958, respectively, should be wired for his benefit to the Cypriot account at Parex-Vilnius through DeutscheBank-New York.

**h. January 28, 2003 and February 23, 2003**

**exchanges in which ICQ User No. 107711 (i.e., the defendant VEGA) admits hacks of credit card information systems to ICQ User No. 100630 (Script).** In a message to ICQ User No. 100630 on January 28, 2003, ICQ User No. 107711 advised that his associates had hacked a database containing dumps on 2 million credit card accounts in the United States.<sup>11</sup> ICQ User No. 107711 proposed selling the dumps to Script and "RyDen." ICQ User No. 100630 replied that the volume was too large for either him or RyDen currently to handle. ICQ User No. 107711 responded that ICQ User No. 100630 and RyDen were "lazy." On or about February 23, 2003 (i.e., three days before the arrest of the defendant in Nicosia), ICQ User No. 107711 sent ICQ User No. 100630 a message urging him to use an enclosed link to a newly published article reporting on what ICQ User No. 107711 emphasized his "boys" had done. The article in question reported that Track Data on 8 million credit

---

<sup>11</sup> Other evidence obtained in this investigation establishes that Script was the user of ICQ No. 100630.

cards had been stolen from Data Processors International ("DPI"). In a follow-up exchange the same day, ICQ User No. 107711 admitted that because the hack by his "guys" had been discovered, he had had to evacuate them to another country. In the same message, ICQ User No. 1007711 also advised that the actual number of credit cards compromised by the theft from DPI was not 8 million, but rather, 14 million, including 450,000 cards issued by CapitalOne.

**B. Evidence That VEGA, "Boa" And  
ICQ User No. 107711 Are One And The Same**

13. As summarized above, the Subject Laptop Computer contains voluminous evidence demonstrating that its owner was a key participant in a scheme that amassed and sold stolen credit card information worldwide. As further explained below, evidence obtained by the Secret Service in the course of its investigation likewise establishes that that owner is in fact the defendant ROMAN VEGA, also known as "Boa", "Roman Stepanenko," "Randy Riolta" and ICQ User No. 107711:

a. The Subject Laptop Computer was secured so that only the owner or one authorized by him could operate it. The operating system was password protected. Moreover, many of the sectors of its hard-drives were encrypted, meaning that files stored on those files, including e-mail logs, long lists of Track

Data and counterfeit passports (see below), could only be accessed by a person who knew the password.

b. The Subject Laptop Computer was recovered from VEGA's hotel room in Nicosia, Cyprus, soon after his arrest on February 26, 2003. Shortly before that seizure, officers had responded to reports of suspiciously large volumes of credit card transactions being processed through a POS terminal at a storefront in Nicosia. At the storefront, the officer observed VEGA swiping numerous cards through a magnetic reader attached to that terminal.

c. The Subject Laptop Computer contains scans of several identity documents bearing VEGA's likeness. These include a Ukrainian passport issued in the name of ROMAN VEGA, a Florida driver's license issued in the name of "Roman Stepanenko," and a Portuguese passport issued in the name of "Randy Riolta" (further discussed below). I have examined each of the three seized images and determined that all depict the same person. Moreover, the man in those three images is also the same person depicted in two other photographs that I have reviewed. The first is one that the United States Marshal maintains on VEGA in connection with the case pending against him in the Northern District of California (see note 5 above) and with another case in which the defendant was arrested in Florida

in 1999.<sup>12</sup> The other photograph is one that the Florida motor vehicles' authority maintains of the person to whom it issued a driver's license in the name "Roman Stepanenko."

d. The Subject Laptop Computer also contains pictures of VEGA's ex-wife, Alena Stepanenko. In an interview with the Postal Inspection Service, Alena Stepanenko admitted that she is the woman in those pictures, as is further confirmed by my comparison of the photos of her on the Subject Laptop Computer to the driver's license photograph that authorities in Florida maintain of her.

e. The e-mail messages recovered from the Subject Laptop Computer to which "Boa" was party, as well as the ICQ chats involving User No. 107711 that were recovered from the same device include numerous instances in which the sender identifies himself alternately as "Roman Vega," "Roman Stepanenko," or "Randy Riolta," and moreover, is addressed by his correspondents as "Roman," or Russian variants thereof. For example:

- In March 2002, the user of ICQ Number 107711 sold hardware and software to be used in the production of credit cards to at least two individuals, both of whom he instructed to send part of his fees to ROMAN VEGA and the remainder to VEGA's ex-wife. In one exchange,

---

<sup>12</sup> The Subject Laptop Computer also contains a copy of the docket report for removal proceeding in the 1999 case, in which the defendant under the name "Roman Stepanenko" was arrested in the Southern District of Florida on a criminal complaint that was then pending in the Eastern District of New York, and that following VEGA's removal here, was dismissed, without prejudice.


ICQ User Number 107711 instructed another ICQ user to send \$1000 via Western Union to Alena Stepanenko in Los Angeles and "the rest" via wire before March 30 to an account in the name of ROMAN VEGA in Brisbane, Australia. In a second exchange, ICQ User Number 107711 instructed a third ICQ user, that with respect to an installment of at least \$3,000 she was about to pay him, she should send "\$1,500 to Los Angeles . . . Alena Stepanenko" and "the rest to [Kiev] Ukraine . . . Roman Vega" (emphasis added);

- On or about September 16, 2002, a person using ICQ No. 100316 (believed to be Script) engaged ICQ User No. 107711 in an exchange about how easy it was to obtain personal information from databases in the United States on individuals living there. To prove the point, ICQ No. 100316 sent ICQ No. 107711 three entries, each listing the full name, date of birth and social security number for Stepanenko, Roman V., accompanied by the remark "Look! The States still remember you" (emphasis added);
- On or about September 19, 2002, a person using the name "Lidia Bekker" sent an e-mail to boa-factory@bk.ru in which she addressed the recipient as "Roman," to which boa-factory@bk.ru responded with a message that he signed "Best Regards, Roman Vega (emphasis added);"
- On or about September 25, 2002, boa-factory@bk.ru sent an e-mail to scaredface@ziplip.com concerning payment owed to him for "186 Visa [dumps]" and "60 MC [Mastercard dumps]" in which he advised "Money- you can send it by Western Union to one of our drop[s]: Randy Riotta, Valetta, Malta" (emphasis added);
- Between September 29, 2002 and October 4, 2002, boa-factory@bk.ru corresponded with dei@zipcom, commissioning "Dei" to forge a marriage certificate between "Roman Vladmirovich Vega" and a woman named "Galya." Boa-factory@bk.ru repeatedly signed his name as "Roman" -- then directed "Dei" to "send me everything," specifying an address for "Roman Vega" in Malta (emphasis added);

- On or about October 24, 2002, "riolta@gmx.co.uk" using an e-mail account automatically formatted with the signature line "Best regards, RR" (i.e., "Randy Riolta"), sent an e-mail to "Lidia Bekker," (see above) that riolta@gmx.co.uk signed "Roman Vega" (emphasis added);
- On or about December 4, 2002, boa-factory@bk.ru sent an e-mail to "variagass@hotmail.com" directing that "if the money is clean" (i.e., not obviously suspicious) "variagass@hotmail.com" should wire payment owed for forgeries of identity documents and credit cards to an account in the name of "Roman Vega" at Bank of Valletta in Malta, but "[i]f the money is dirty, then I'll give you another account."

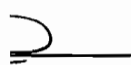
### III. Conclusion

WHEREFORE, your deponent requests that a warrant be issued directing the arrest of the defendant ROMAN VEGA, also known as "Boa", "Roman Stepanenko," "Randy Riolta" and ICQ User No. 107711, so that he may be dealt with according to the law and it is further respectfully requested that this Affidavit and the resulting warrant be sealed until such time as the defendant has been apprehended.

  
\_\_\_\_\_  
HARI NOTANI  
Special Agent  
United States Secret Service

Sworn to before me this  
24th day of August, 2007

\_\_\_\_\_  
THE  
UNIT  
EAST

  
\_\_\_\_\_  
MOTO  
JUDGE  
YORK